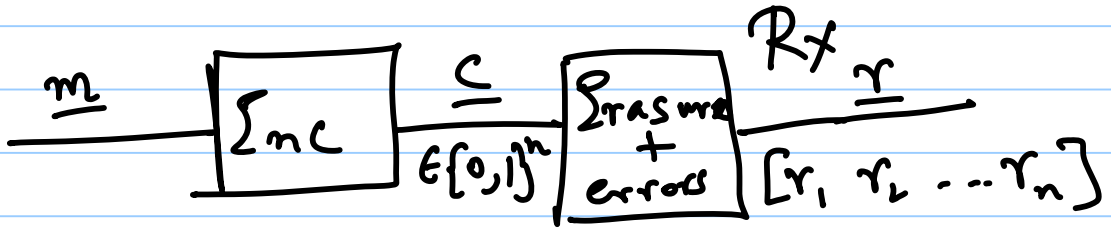
Binary BCH Codes

Note Title

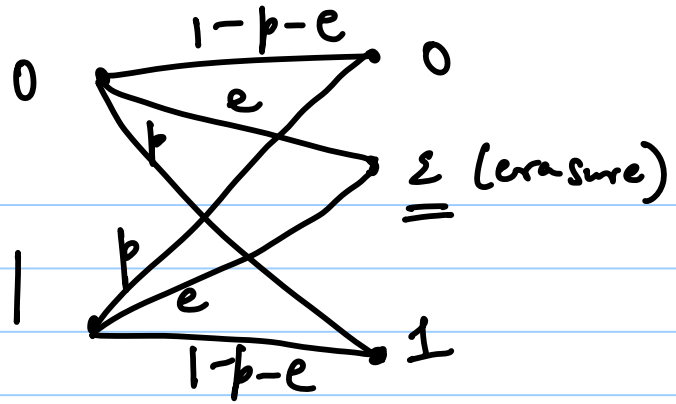
- PC matrix → generator matrix
- Encoding
- Decoding

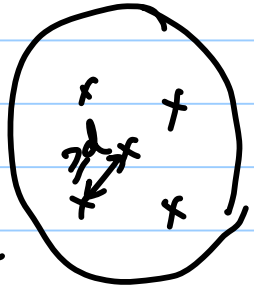
} can be implemented

Erasures + Errors decoding



$r_i \in \{0, 1, \varepsilon\}$





No erasure $\begin{cases} d_{min} = d \Rightarrow t : 2t+1 \leq d \\ \text{errors} \\ \text{can be corrected.} \end{cases}$

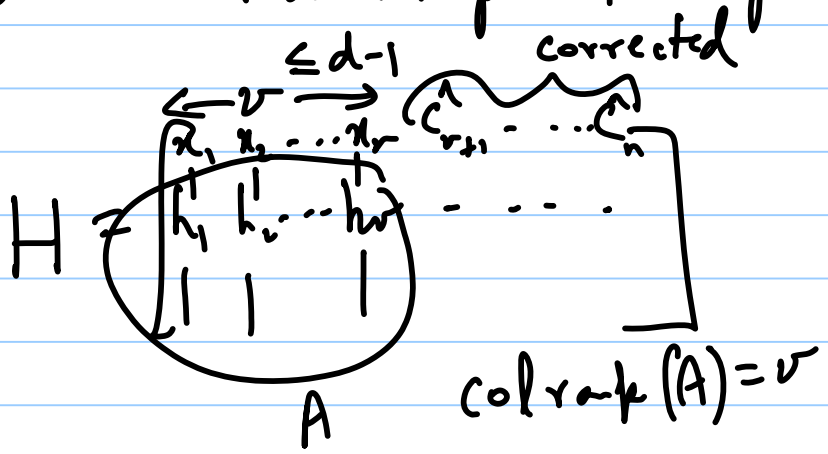
Erasure + error model $\begin{cases} u \text{ errors and } v \text{ erasures are correctable} \\ \text{whenever } 2u + v + 1 \leq d \end{cases}$

Pf: 1st step: puncture the code to remove ν erased positions.

$$d_{min}(\text{punctured code}) \geq d-\nu$$

Since $2u+1 \leq d-\nu$, u errors can be corrected in punctured part

2nd step:



$$H \begin{bmatrix} x_1 \\ \vdots \\ x_r \\ \hat{c}_{r+1} \\ \vdots \\ \hat{c}_n \end{bmatrix} = \underline{0}$$

know this

$$A \begin{bmatrix} x_1 \\ \vdots \\ x_r \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_{n-k} \end{bmatrix}$$

unknown

BCH decoding:

u errors + v erasures

$(2u+v+1 \leq d)$

How to adapt algebraic bounded distance decoder?

$$u + \frac{v}{2} \leq t = \frac{d-1}{2}$$

1) Put erased bits = 0, do algebraic decoding
2) Put " " = 1, " " "

Cyclic codes:

BCH codes: $n = \text{ord}(\beta)$, $\beta \in GF(2^m)$

(n: odd)

$d = 2t+1$

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \\ 1 & \beta^2 & \beta^4 & \cdots & (\beta^2)^{n-1} \\ \vdots & & & & \\ 1 & \beta^{2t} & (\beta^{2t})^2 & \cdots & (\beta^{2t})^{n-1} \end{bmatrix}$$

$\underline{c} = [c_0 \; c_1 \; c_2 \cdots c_{n-1}] \in \text{Code}$

$\updownarrow$

$\underline{c}' = [c_{n-1} \; c_0 \; c_1 \cdots c_{n-2}] \in \text{Code}$

Code is cyclic.

$\text{ord}(\beta) > n$ $\xleftarrow{?}$ shorten

$\downarrow$

define BCH code with length $= \text{ord}(\beta)$

Cyclic codes: linear codes closed under cyclic right (left) shift

- binary, n: odd.

Ring, R_n: $\{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} : a_i \in \{0,1\}\}$

$x \bmod (x^n + 1)$

$c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in R_n$

$x\,c(x) = c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1} \in R_n$

Ideal of R_n: $I \subseteq R_n$ is an ideal

if (1) $a(x), b(x) \in I$,

then $a(x) + b(x) \in I$

(2) $a(x) \in I$, $b(x) \in R_n$

$b(x)\,a(x) \in I$

$b_0 + b_1 x + b_2 x^2 + \cdots + b_{n-1} x^{n-1}$

I: ideal $\Rightarrow$ $x\,a(x) \in I$ $\circ$

$a(x) \in I$

→ Binary cyclic codes are ideals of R_n.

Ex of ideal:

Fix $g(x) \in R_n$

$I = \{ a(x)\, g(x) : a(x) \in R_n \}$ is an ideal.

$= \langle g(x) \rangle$ — principal ideals.

Result: C: cyclic code of length n (n: odd)

(1) Let $g(x)$: nonzero poly in C with minimal degree.

Then, $g(x)$ is unique.

(2) $C = \langle g(x) \rangle$

Pf: Let $c(x) \in C$.

Divide $c(x)$ by $g(x)$ in $GF(2)[x]$

$$c(x) = q(x)g(x) + r(x) \qquad \deg r(x) < \deg g(x)$$

$$c(x) + q(x)g(x) = r(x) \in C$$

$c(x) \in C$ $\quad$ $q(x)g(x) \in C$ $\quad$ $r(x) = 0$

(3) $g(x) \mid (x^n + 1)$ in $GF(2)[x]$.

$g(x)$: generator polynomial of cyclic code.